REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks. Claims 16, 18-21, and 23-31 are currently pending.

Claim Rejections Under 35 U.S.C. § 103

Claims 16, 18-21 and 23-31 are rejected under 35 U.S.C. §103(a) on the basis of Watanabe et al (U.S. Patent Application Publication No. 2002/0069361, hereinafter "Watanabe") in view of Yamaguchi et al (U.S. Patent Application Publication No. 2001/0036301 hereinafter "Yamaguchi"). This rejection is traversed as follows.

Claim 16 recites a method of securing access to a piece of equipment, the method comprising, *inter alia*,

> storing an encrypted version of said authentic biometric signature on said piece of equipment; ...
> transmitting, from said piece of equipment, said encrypted biometric signature to an authentication medium comprising an electronic chip card that is separate from said piece of equipment; ...
> verifying, in said authentication medium, the authenticity of [a] plain biometric signature by comparing said plain biometric signature ... with said ... authentic biometric signature ...; and
> granting said user access to said piece of equipment if said comparison is successful ...

Thus, according to claim 16, there are two elements of structure involved, namely a piece of equipment to which access is to be granted, and an authentication medium that performs a comparison of an authentic version of a biometric signature that has been encrypted with a plain biometric signature that has been obtained. Moreover, the authentic version of the biometric signature is stored on the piece of

equipment whose access is being controlled, and is transmitted from the piece of equipment to the authentication medium. The authentic signature is transmitted in encrypted form, so that it remains secure, and decrypted at the authentication medium. With this arrangement, if different sets of people have access rights to different respective pieces of equipment, it is only necessary to store the biometric data for each authorized user in the associated pieces of equipment, in a decentralized manner.

The Office Action mainly relies upon paragraphs 0335, 0356 and 0357 of the Watanabe reference as allegedly disclosing the above-recited features. See the Office Action: pages 6 and 7, reasons for rejecting claim 16. Paragraph 0335 of the Watanabe reference pertains to the embodiment illustrated in Figure 24 of the patent. The paragraph begins by stating "A user device can include both an IDC and a PKC, for example, when the user device is designed to execute a process of comparing sampling information with a template included in a person identification certificate (IDC)". As shown in Fig. 24 of Watanabe, the IDC is stored in the UD (user device), and a comparison between the sampling information and the IDC is performed by the UD to determine if access to the UD is granted.

Paragraphs 0356 and 0357 of the Watanabe reference pertain to the embodiment of Fig. 27. Preceding paragraph 0355 states "Fig. 27 is a diagram illustrating a system in which verification is performed by a personal terminal such as an IC card using a person identification certificate (IDC) stored in the personal terminal and only the result of the verification is transmitted to a shared user device."

Thus, in both of the embodiments of the Watanabe reference that are indicated in the Office Action, the IDC is stored in the same device that performs the

verification. As such, there is no reason to transmit the encrypted personal identification information, e.g. the IDC, from that device to another medium to perform the verification, nor any disclosure of such an operation. Moreover, this lack of disclosure is recognized in the Office Action. On page 6, in the comparison of claim 16 to the Watanabe patent, the Action omits the "transmitting" step that is recited in the claim.

To address this difference between the disclosure of the Watanabe patent and claim 16, the Office Action refers to Figure 42 of the Yamaguchi patent, as well as paragraphs 0040 and 0044-0046 of that patent. In relevant part, these portions of the patent describe a fingerprint checking device 411 in which registered fingerprint data can be stored in a storage unit 414 that is part of the device. Alternatively, it can be stored on a hard disk drive 425 of a host computer 420 connected to the device, or an IC card 431 that interfaces with the host computer, and downloaded to the device. The hard disk drive and the IC card essentially function as auxiliary storage mechanisms for the fingerprint checking device.

The Office Action relies upon this disclosure to support the conclusion that, "if the encrypted biometric sample is stored on the computer, and [another device] is performing the comparison, then the encrypted biometric sample must be sent to the [other device]". Office Action at page 7. However, this teaching is not sufficient to render the claimed subject matter obvious. Unlike the recitations of claim 16, the computer 420 in the Yamaguchi patent is not "said piece of equipment" to which access is granted if the comparison is successful, i.e. the device being controlled. Rather, as disclosed in paragraph 0041 of the Yamaguchi patent, the control unit 413 of the fingerprint checking device performs the comparison, "and if they match,

control of unlocking or the like is made according to an output signal from the control unit 413." There is no disclosure that this output signal controls access to the computer 420 that stores the fingerprint data. Rather, it is sent to another device, e.g. an electric lock for entrance to a room.

Thus, the Yamaguchi patent does not disclose a method or system for securing access to a piece of equipment in which an encrypted biometric signature is stored "on said piece of equipment", and is transmitted "from said piece of equipment" to an authentication medium that performs a comparison of signatures, and wherein "access to said piece of equipment" is granted if the comparison is successful, as recited in the independent claims. Likewise, the Watanabe patent does not disclose that an encrypted biometric signature is stored on a piece of equipment whose access is being controlled, and is transmitted from that piece of equipment to another device for verification purposes. Consequently, any reasonable combination of the teachings of these two references would not lead a person of ordinary skill in the art to the claimed subject matter. Rather, the logical combination would be either to store the biometric signature information on the same device that is performing the comparison, or to store it on a computer or IC card that is different from the device being controlled, and download it to the device which is performing the comparison. Neither of these results is the same as what is being claimed.

At page 4, the Office Action asserts:

> There are two entities which can perform the authentication (IC card or device) and there are two places where the authenticated biometric data can be stored (IC card or the device). Therefore, four finite combinations are present and one of ordinary skill in the art could have tried any of them. Yamaguchi was also shown to teach why one of ordinary skill in the art might have

> chosen the combination present in the claimed invention. Since IC cards traditionally have limited memory, a computer device could store many encrypted biometric templates in a hard drive in a very efficient manner.

However, in the Yamaguchi patent, the computer device on which the biometric templates are stored is not the piece of equipment whose access is being controlled. It is respectfully submitted that this feature of the claimed subject matter is being overlooked in the foregoing analysis.

In view of the foregoing, claim 16 is submitted to be patentable over the prior art of record. For similar reasons, it is respectfully submitted that the references do not suggest the subject matter of independent claims 21 or 26, or any of the claims depending therefrom.

CONCLUSION

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 15, 2011

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839
703 836 6620